



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/558,022	04/25/2000	Takatoshi Ono	NAK1-BK74	9324
21611	7590	10/17/2005	EXAMINER	
SNELL & WILMER LLP 600 ANTON BOULEVARD SUITE 1400 COSTA MESA, CA 92626			SHERKAT, AREZOO	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 10/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/558,022	Applicant(s) ONO ET AL.	
	Examiner Arezoo Sherkat	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 August 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Response to Amendment

This office action is responsive to Applicant's amendment received on August 1, 2005. Claims 1-10 are pending.

Response to Arguments

Applicant's arguments filed on August 1, 2005 have been fully considered but they are not persuasive.

Applicant argues that "Wasilewski does not disclose a data usage controlling apparatus that decrypts the encrypted condition information using the type 2 key and includes second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key".

Examiner responds that Wasilewski discloses that MSK (i.e., type 1 key) changes/updates in the order of once a day or once a month in SABER 20 to be transferred to STU 90 (Col. 10, lines 1-12). Wasilewski also discloses encrypting the new type 2 key (i.e., control words that are used in the first level of encryption and are changed every few seconds - Col. 8, lines 48-60) using the updated type 1 key (i.e., MSK that are updated in the order of once a day or once a month – Col. 10, lines 1-5) and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key (Col. 9, lines 12-67 and Col. 10, lines 13-67).

Examiner respectfully maintains the rejection formulated on April 4th, 2005 as follows:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6 and 9-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Wasilewski et al., (U.S. Patent No. 5,870,474 and Wasilewski hereinafter).

Regarding claims 1-2 and 9-10, Wasilewski discloses a data usage controlling method that

(1) reads a type 1 key (i.e., MSK) from a storage unit and (a) main data (i.e., payload), (b) an encrypted type 2 key produced by encrypting a type 2 key (i.e., random number generated keys, referred to hereinafter as control words) using the type 1 key, and (c) encrypted condition information produced by encrypting condition information using the type 2 key from a recording medium (Col. 8, lines 1-47),

(2) decrypts the encrypted condition information using the type 2 key (Col. 9, lines 47-58), and

(3) controls usage of the read main data base on the condition information, the data usage controlling method comprising the following steps: updating the condition information in accordance with usage of the main data (Col. 8, lines 48-60);

generating a new type 2 key in accordance with the usage of the main data, and encrypting the updated condition information using the new type 2 key and replacing the encrypted condition information on the recording medium with the encrypted updated condition information (Col. 8, lines 22-60);

updating the type 1 key in accordance with the usage of the main data (Col. 10, lines 1-12); and

encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key (Col. 9, lines 12-67 and Col. 10, lines 13-67).

Regarding claim 3, Wasilewski discloses a data usage controlling apparatus further comprising:

second updating means for updating the condition information in accordance with usage of the read main data (Col. 10, lines 1-12); and

wherein the first encrypting means encrypts the updated condition information using the new type 2 key and replaces the encrypted condition information on the recording medium with the encrypted updated condition information (Col. 9, lines 12-67 and Col. 10, lines 13-67).

Regarding claim 4, Wasilewski discloses a data usage controlling apparatus wherein the generating means generates a new type 2 key every time a user makes a predetermined number of uses of the main data on the recording medium, and when the

Art Unit: 2131

generating means has not generated a new type 2 key, the first encrypting means re-encrypts the updated condition information using a same type 2 key as was used to decrypt the encrypted condition information (Col. 8, lines 7-47 and Col. 10, lines 1-12).

Regarding claim 5, Wasilewski discloses a data usage controlling apparatus wherein the main data in each set on the recording medium has been encrypted using a type 3 encryption key, the data usage controlling apparatus further comprising:

obtaining means for obtaining the type 3 encryption key, and second decrypting means for decrypting the read main data using the obtained type 3 encryption key (Col. 10, lines 13-67 and Col. 11, lines 1-9).

Regarding claim 6, Wasilewski discloses a data usage controlling apparatus wherein the main data in each set on the recording medium has been encrypted using a type 3 encryption key that is unique to the data usage controlling apparatus (i.e., public key corresponding to STU's private key), the data usage controlling apparatus further comprising:

storing means for storing the type 3 encryption key, and second decrypting means for decrypting the read main data using the stored type 3 encryption key (Col. 10, lines 43-67 and Col. 11, lines 1-9).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al., (U.S. Patent No. 5,870,474 and Wasilewski hereinafter), in view of Dillon, (U.S. Patent No. 5,659,615).

Teachings of Wasilewski with respect to claim 2 have been discussed previously.

Regarding claims 7-8, Wasilewski does not expressly disclose a data usage controlling apparatus wherein the updating means updates the type 1 key by performing a predetermined calculation on the read type 1 key.

However, Dillon discloses a data usage controlling apparatus wherein the updating means updates the type 1 key by performing a predetermined calculation on the read type 1 key (i.e., each key sequence number is one more than its previous key sequence number)(Col. 5, lines 15-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the data usage controlling system of Wasilewski by including wherein the updating means updates the type 1 key by adding one to the read type 1 key as disclosed by Dillon. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the

suggestion of Dillon to provide for the system to change the keys frequently and allow only an authorized receiver access to the keys (Dillon, Col. 6, lines 17-30).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Arezoo Sherkat
Patent Examiner
Group 2131
Oct. 12, 2005



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100